

**RECEIVED  
CENTRAL FAX CENTER**

NOV 01 2004

**ZILKA KOTAB**  
PC  
ZILKA, KOTAB & FEECE™95 SOUTH MARKET ST., SUITE 420  
SAN JOSE, CA 95113TELEPHONE (408) 971-2573  
FAX (408) 971-4660**FAX COVER SHEET**

<b>Date:</b> November 1, 2004	<b>Phone Number</b>	<b>Fax Number</b>
<b>To:</b> Board of Patent Appeals & Interferences		(703) 872-9306
<b>From:</b> Kevin J. Zilka		

**Docket No.:** NATIP003\_00.069.01**App. No:** 09/586,265**Total Number of Pages Being Transmitted, Including Cover Sheet:** 30**Message:**

Please deliver to the Board of Patent Appeals &amp; Interferences.

Thank you,

Kevin J. Zilka

☐ Original to follow Via Regular Mail ☒ Original will Not be Sent ☐ Original will follow Via Overnight Courier

\*\*\*\*\*  
The information contained in this facsimile message is attorney privileged and confidential information intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copy of this communication is strictly prohibited. If you have received this communication in error, please immediately notify us by telephone (if long distance, please call collect) and return the original message to us at the above address via the U.S. Postal Service. Thank you.  
\*\*\*\*\*

IF YOU DO NOT RECEIVE ALL PAGES OR IF YOU ENCOUNTER  
ANY OTHER DIFFICULTY, PLEASE PHONE Erica  
AT (408) 971-2573 AT YOUR EARLIEST CONVENIENCE

November 1, 2004

**RECEIVED  
CENTRAL FAX CENTER**

NOV 01 2004

Practitioner's Docket No. NAIIP003/00.069.01

PATENT

## IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Edwards et al.

Application No.: 09/586,265

Group No.: 2134

Filed: 05/31/2000

Examiner: Tran, T.

For: SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR SELECTING VIRUS  
DETECTION ACTIONS BASED ON A PROCESS BY WHICH FILES ARE BEING ACCESSED

Mail Stop Appeal Briefs – Patents

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF  
(PATENT APPLICATION--37 C.F.R. § 1.192)

1. Transmitted herewith is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on October 28, 2004.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

## CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10\*

*(When using Express Mail, the Express Mail label number is mandatory;  
Express Mail certification is optional.)*

I hereby certify that, on the date shown below, this correspondence is being:

## MAILING

deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)  
with sufficient postage as first class mail.37 C.F.R. § 1.10\*  
as "Express Mail Post Office to Addressee"  
Mailing Label No. \_\_\_\_\_ (mandatory)

## TRANSMISSION

✓ facsimile transmitted to the Patent and Trademark Office, (703) 872-9306.

  
Signature

Date: 11/1/2004

Erica L. Farlow

(type or print name of person certifying)

\* Only the date of filing (1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under 1.3 continues to be taken into account in determining timeliness. See 1.703(f). Consider "Express Mail Post Office to Addressee" (1.10) or facsimile transmission (1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.

Transmittal of Appeal Brief--page 1 of 2

**3. FEE FOR FILING APPEAL BRIEF**

Pursuant to 37 C.F.R. § 1.17(c), the fee for filing the Appeal Brief is:

other than a small entity \$340.00

**Appeal Brief fee due \$340.00**

**4. EXTENSION OF TERM**

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

**5. TOTAL FEE DUE**

The total fee due is:

Appeal brief fee \$340.00

Extension fee (if any) \$0.00

**TOTAL FEE DUE \$340.00**

**6. FEE PAYMENT**

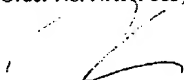
Authorization is hereby made to charge the amount of \$340.00 to Deposit Account No. 50-1351 (Order No. NA11P003).

A duplicate of this transmittal is attached.

**7. FEE DEFICIENCY**

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NA11P003).

Reg. No.: 41,429  
Tel. No.: 408-971-2573  
Customer No.: 28875

  
\_\_\_\_\_  
Signature of Practitioner  
Kevin J. Zilka  
Zilka-Kotab, PC  
P.O. Box 721120  
San Jose, CA 95172-1120  
USA

Transmittal of Appeal Brief—page 2 of 2

**RECEIVED  
CENTRAL FAX CENTER**

**NOV 01 2004**

**PATENT**

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of:	)
	)
Edwards et al.	) Art Unit: 2134
	)
Application No. 09/586,265	) Examiner: Tran, T.
	)
Filed: 5/31/2000	) Date: 11/01/04
	)
For: SYSTEM, METHOD AND COMPUTER	)
PROGRAM PRODUCT FOR SELECTING	)
VIRUS DETECTION ACTIONS BASED ON	)
A PROCESS BY WHICH FILES ARE BEING	)
ACCESSED	)

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**ATTENTION: Board of Patent Appeals and Interferences**

**APPELLANT'S BRIEF (37 C.F.R. § 41.37)**

This brief is in furtherance of the Notice of Appeal, filed in this case on October 28, 2004.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

- I REAL PARTY IN INTEREST
- II RELATED APPEALS AND INTERFERENCES

NA11P003/00.069.01

- 1 -

- III STATUS OF CLAIMS
- IV STATUS OF AMENDMENTS
- V SUMMARY OF CLAIMED SUBJECT MATTER
- VI ISSUES
- VII ARGUMENTS
- VIII APPENDIX OF CLAIMS INVOLVED IN THE APPEAL
- IX APPENDIX LISTING ANY EVIDENCE RELIED ON BY THE APPELLANT IN THE APPEAL

The final page of this brief bears the practitioner's signature.

**1 REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))**

The real party in interest in this appeal is Networks Associates Technology, Inc.

## II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c))

### (1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals, interferences, or related judicial proceedings.

Since no such proceedings exist, no Related Proceedings Appendix is appended hereto.

**III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))****A. TOTAL NUMBER OF CLAIMS IN APPLICATION**

Claims in the application are: 1-20

**B. STATUS OF ALL THE CLAIMS IN APPLICATION**

1. Claims withdrawn from consideration: none
2. Claims pending: 1-20
3. Claims allowed: None
4. Claims rejected: 1-20

**C. CLAIMS ON APPEAL**

The claims on appeal are: 1-20

See additional status information in the Appendix of Claims.



#### IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, there are no such amendments after final.

**V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. §  
41.37(c)(1)(v))**

With respect to a summary of Claim 1 et al., as shown in Figure 2, a process is identified, in operation 204, for accessing files and selecting virus detection actions based at least in part on the identified process if no identifier is assigned thereto. Note operation 206. A description of an exemplary, optional embodiment of such operations may be found on lines 10-30 on page 7 of the originally filed application. Turning to Figure 3, an identifier is assigned to the process if no identifier is assigned thereto. See operation 306. As noted in operation 308, virus detection actions are selected based at least in part on the identifier if existent. A description of an exemplary, optional embodiment of such operations in Figure 3 may be found on page 8 of the originally filed application. Still yet, turning back to Figure 2, the virus detection actions are performed on the files, as noted in operation 208. During use, the process is associated with an application program, and different identifiers are assigned to different application programs so that the virus detection actions are tailored for the processes associated with the application programs.

**VI ISSUES (37 C.F.R. § 41.37(c)(1)(vi))**

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has rejected Claims 1-20 under 35 U.S.C. 102(b) as being anticipated by Chen et al. (U.S. Patent No. 5,960,170).

## VII ARGUMENTS (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.


### Issue #1:

The Examiner has rejected Claims 1-20 under 35 U.S.C. 102(b) as being anticipated by Chen et al. (U.S. Patent No. 5,960,170).

### *Group #1: Claims 1, 6-7, 12-13, and 18*

In particular, the Examiner relies on Fig. 4C-4D; col. 11, line 51 – col. 13, line 23; and col. 19, line 39 – col. 20, line 6 of Chen to make a prior art showing of appellant's claimed "identifying a process for accessing files and selecting virus detection actions based at least in part on the identified process..." (see all of the independent claims).

Appellant has carefully reviewed the foregoing excerpts along with the remaining Chen reference. During the course of such careful review, appellant notes that there is simply no identification of an application program-related "process for accessing files and selecting virus detection actions based at least in part on the identified process." In sharp contrast, Chen merely suggests selecting virus detection actions *based on file types*. See Figure 4C from Chen below, for example.



Media	Virus type	Virus name
1	File type (e.g. .exe, .com)	Virus A
2	Application data file (e.g. .doc)	Virus B
3	File type	Virus C
4	Applet (e.g. Java)	Virus D
5	File type	Virus E
6	File type	Virus F

Fig. 4C

Further, this assertion is further corroborated by Chen's specific examples below:

"if the scanning scope is indicated by the request for virus scanning, scan according to the request";

"if the scanning scope is not indicated by the request, determine whether the client includes writable media";

"if client does not include writable media, then do not perform virus scan";

"if a related scan detected Virus X, then scan client for Virus X";

"if the client includes a hard disk, then scan according to the conditions specific to the hard disk";

"if .exe files are present, then perform file virus signature scan",

"if .com files are present, then perform file virus signature scan",

"if application data files are present, then scan for macro viruses",

"if the client is a postal node, then scan all unread messages for attachments",

"if the client has received electronic mail, scan unencoded portions thereof", and

"if client includes a Java applet execution engine, then scan for hostile Java applets";

"if the client includes other writable media, then determine the conditions specific to the writable media and scan the writable media." (col. 23, lines 1-26)

Only appellant teaches and claims the specific selection of virus detection actions based on an application program process for accessing files, in order provide tailored virus detection actions *based on an application program that is accessing a file*.

Still yet, it is further noted that the foregoing excerpts and the remaining Chen reference fail to meet appellant's claimed "identifying a process for accessing files and selecting virus detection actions based at least in part on the identified process if no identifier is assigned thereto," "assigning an identifier to the process if no identifier is assigned thereto" and "selecting virus detection actions based at least in part on the identifier if existent" (emphasis added – see all independent claims).

There is simply no identification of an application program process for accessing files on the condition that no identifier is assigned thereto, and assigning an identifier to the process if no identifier is assigned thereto, wherein virus detection actions are selected based at least in part on the identifier if existent.

As set forth on page 4 of the originally filed specification, use of the application program process-specific identifier allows virus detection actions to be selected based on the identifier for accelerating the selection process. Thus, the present claimed invention need not identify the application program process, since the identifier (when available) is used to select the virus detection actions. By employing the identifier, the technique of selecting the virus detection actions based on the identification and analysis of the process may be avoided. Further, if the application program process-specific identifier is nonexistent, the claimed invention provides that an identifier is assigned thereto so that the technique of selecting the virus detection actions based on the identification and analysis of the process may be avoided the next time the application program process attempts to access a file.

Still yet, the Examiner relies on col. 4, lines 15-30; col. 12, lines 12-35; and col. 13, lines 1-23 of Chen to make a prior art showing of appellant's claimed "process is associated with an application program, and different identifiers are assigned to

different application programs so that the virus detection actions are tailored for the processes associated with the application programs.”

Again, Chen does not disclose, teach or even suggest any sort of application program process-specific identifiers, but rather merely “virus identifiers.” See, for example, Fig. 4C of Chen and the accompanying description.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.* 868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Chen reference, in view of the stark deficiencies noted above.

In the Examiner's latest response mailed 10/19/04, the Examiner responds to appellant's arguments above regarding the following limitations: “wherein the process is associated with an application program, and different identifiers are assigned to different application programs so that the virus detection actions are tailored for the processes associated with the application programs.” Specifically, the Examiner asserts that “Chen teaches in the cited portion of [the] prior art that the server is performing the detection of viruses requested by the client and each virus detection routine is tailored according to different types of files. The limitation is met because in order for the server to determine which routine to access, the server must determine what type of application it is accessing in order to identify the detection routine [that] tailors to that particular application.”

Appellant respectfully disagrees with this assertion. Specifically, with respect to the Examiner's first statement, it appears that the Examiner is agreeing with appellant's previous arguments that Chen merely suggests selecting virus detection actions *based on file types*, in contrast to appellant who teaches and claims the specific selection of virus detection actions based on an application program process for accessing files, in order to provide tailored virus detection actions *based on an application program that is accessing a file*.

However, from the Examiner's second statement above, it appears that the Examiner is now asserting that the aforementioned claimed subject matter is *inherently* taught by Chen. Appellant respectfully disagrees with such assertion. Specifically, the server in Chen does not need to determine what type of application it is accessing in order to identify the detection routine that tailors to that particular application. Instead, Chen merely utilizes file extensions for selecting virus detection actions *based on file types*. Supporting this assertion is the following excerpt from Chen.

"For example, separate routines for the detection of viruses that could reside in systems using particular platforms and operating systems, in particular file types, and in particular locations are provided for separate access in the scanning module 454. Specifically, routines for the detection of viruses that typically reside on one platform are provided such that they can be accessed separate from routines for the detection of viruses that typically reside on another platform. Similarly, routines for the detection of viruses that reside in "executable" files (such as those that have the file extension .exe) are provided such that they can be accessed separate from routines used for the detection of macro viruses (such as those that implement the WordBasic programming language, typically reside in application data files, and include extensions such as .doc or .dot). Thus, a virus detection routine that examines a file to determine whether it includes a virus signature can be separated from a virus detection routine that use a set of rules, such as combinations of suspect instructions, to determine whether viruses are present in files. Other types of virus detection routines can be provided in the scanning module 454, such as those used in the detection of viruses in electronic mail messages." (col. 11, lines 29 - 51)

It appears that the Examiner has relied on an inherency argument regarding the above emphasized claim limitations. In view of the arguments made hereinabove,



any such inherency argument has been adequately rebutted, and a notice of allowance or a specific prior art showing of such claim features, in combination with the remaining claim elements, is respectfully requested. (See MPEP 2112)

Irregardless of the above issue, the Examiner has not yet addressed appellant's previous arguments regarding the claimed "identifying a process for accessing files and selecting virus detection actions based at least in part on the identified process if no identifier is assigned thereto," "assigning an identifier to the process if no identifier is assigned thereto" and "selecting virus detection actions based at least in part on the identifier if existent" (emphasis added – see all independent claims).

Still yet, the Examiner has not addressed the plethora of previously-submitted arguments appellant has made with respect to the deficiencies in the Examiner's rejection of the dependent claims.

A notice of allowance or a specific prior art showing of such claimed features, in combination with the remaining claim elements, is respectfully requested.

*Group #2: Claims 2, 8, and 14*

With respect to the present group, the Examiner relies on the following excerpt from Chen to make a prior art showing of appellant's claimed "wherein the identifier is cleared upon the occurrence of a predetermined event."

"Various types of scanning are implemented for efficient iterative analysis. An preferred technique which allows exhaustive signature scanning without requiring a comprehensive download of the signature data is described with reference to FIG. 4D above. Other scanning techniques are also provided for iterative virus detection. For example, techniques for the determination of whether a macro includes a virus can be modularized or divided into a plurality of functions which can be performed by separate virus detection objects. To explain, in the detection of known and unknown viruses in macros, combinations of suspect instructions can be used in the determination of whether a file includes a virus. Specifically, a macro that includes both a first suspect instruction and a second suspect instruction can be determined

to include an unknown (or known) virus. Thus, in accordance with the present invention, separate virus detection objects are provided to first detect whether and which of several targeted files include a first suspect instruction, and then to determine whether those targeted files that include the first suspect instruction also include the second suspect instruction to detect a virus. To produce a first virus detection object the 1VDM 450a operates with the scanning module 454 and the virus rules module 458 to obtain the routines and data required for the detection of the first suspect instruction. After transmission of the first virus detection object from the virus detection server 400 to the client 300 and execution by the client 300, identification of those files that include the first suspect instruction can be identified in the results transmitted to the virus detection server 400. Alternatively, the file identifiers can remain at the client 300 and the result could indicate which suspect instruction was identified. In either case, the virus detection server 400 can use the results to produce an additional virus detection object to determine whether the second suspect instruction is present." (col. 19, line 39 - col. 20, line 6)

Appellant respectfully disagrees with this assertion. After reviewing the above excerpt, and the remaining Chen reference, it is clear that Chen fails to disclose, teach, or even suggest any sort of "identifier [that] is cleared upon the occurrence of a predetermined event" (emphasis added), let alone such functionality applied to an application program-process specific identifier, as claimed. Only appellant teaches and claims the clearance of the application program-process specific identifier, as claimed, upon the occurrence of a predetermined event, so that it may be reused, for example, with other application programs for a similar purpose.

Again, the anticipation criterion has simply not been met by the Chen reference, in view of the stark deficiencies noted above. A notice of allowance or a specific prior art showing of such claimed features, in combination with the remaining claim elements, is respectfully requested.

*Group #3: Claims 3, 9, and 15*

With respect to Claims 3, 9, and 15, the Examiner relies on the following excerpt from Chen to make a prior art showing of appellant's claimed "wherein the identifier is reused after being cleared."

"Various types of scanning are implemented for efficient iterative analysis. An preferred technique which allows exhaustive signature scanning without requiring a comprehensive download of the signature data is described with reference to FIG. 4D above. Other scanning techniques are also provided for iterative virus detection. For example, techniques for the determination of whether a macro includes a virus can be modularized or divided into a plurality of functions which can be performed by separate virus detection objects. To explain, in the detection of known and unknown viruses in macros, combinations of suspect instructions can be used in the determination of whether a file includes a virus. Specifically, a macro that includes both a first suspect instruction and a second suspect instruction can be determined to include an unknown (or known) virus. Thus, in accordance with the present invention, separate virus detection objects are provided to first detect whether and which of several targeted files include a first suspect instruction, and then to determine whether those targeted files that include the first suspect instruction also include the second suspect instruction to detect a virus. To produce a first virus detection object the IVDM 450a operates with the scanning module 454 and the virus rules module 458 to obtain the routines and data required for the detection of the first suspect instruction. After transmission of the first virus detection object from the virus detection server 400 to the client 300 and execution by the client 300, identification of those files that include the first suspect instruction can be identified in the results transmitted to the virus detection server 400. Alternatively, the file identifiers can remain at the client 300 and the result could indicate which suspect instruction was identified. In either case, the virus detection server 400 can use the results to produce an additional virus detection object to determine whether the second suspect instruction is present." (col. 19, line 39 - col. 20, line 6)

Appellant respectfully disagrees with this assertion. After reviewing the above excerpt, and the remaining Chen reference, it is clear that Chen fails to disclose, teach, or even suggest any sort of "identifier [that] is reused after being cleared" (emphasis added), let alone such functionality applied to an application program-process specific identifier, as claimed. Only appellant teaches and claims the reuse of an application program-process specific identifier, as claimed.

Again, the anticipation criterion has simply not been met by the Chen reference, in view of the stark deficiencies noted above. A notice of allowance or a specific prior art showing of such claimed features, in combination with the remaining claim elements, is respectfully requested.

*Group #4: Claims 4, 10, and 16*

With respect to the present group, the Examiner again relies on the following excerpt from Chen to make a prior art showing of appellant's claimed "wherein the event is the termination of an application."

"Various types of scanning are implemented for efficient iterative analysis. An preferred technique which allows exhaustive signature scanning without requiring a comprehensive download of the signature data is described with reference to FIG. 4D above. Other scanning techniques are also provided for iterative virus detection. For example, techniques for the determination of whether a macro includes a virus can be modularized or divided into a plurality of functions which can be performed by separate virus detection objects. To explain, in the detection of known and unknown viruses in macros, combinations of suspect instructions can be used in the determination of whether a file includes a virus. Specifically, a macro that includes both a first suspect instruction and a second suspect instruction can be determined to include an unknown (or known) virus. Thus, in accordance with the present invention, separate virus detection objects are provided to first detect whether and which of several targeted files include a first suspect instruction, and then to determine whether those targeted files that include the first suspect instruction also include the second suspect instruction to detect a virus. To produce a first virus detection object the IVDM 450a operates with the scanning module 454 and the virus rules module 458 to obtain the routines and data required for the detection of the first suspect instruction. After transmission of the first virus detection object from the virus detection server 400 to the client 300 and execution by the client 300, identification of those files that include the first suspect instruction can be identified in the results transmitted to the virus detection server 400. Alternatively, the file identifiers can remain at the client 300 and the result could indicate which suspect instruction was identified. In either case, the virus detection server 400 can use the results to produce an additional virus detection object to determine whether the second suspect instruction is present." (col. 19, line 39 - col. 20, line 6)

Appellant respectfully disagrees with this assertion. After reviewing the above excerpt, and the remaining Chen reference, it is clear that Chen fails to disclose, teach, or even suggest any sort of clearance of the application program-process specific identifier specifically at "the termination of an application." Only appellant teaches and claims such a feature.

Yet again, the anticipation criterion has simply not been met by the Chen reference, in view of the stark deficiencies noted above. A notice of allowance or a specific prior art showing of such claimed features, in combination with the remaining claim elements, is respectfully requested.

*Group #5: Claims 5, 11, and 17*

With respect to the present group, the Examiner again relies on the following excerpt from Chen to make a prior art showing of appellant's claimed "wherein the identifier is assigned by the application."

"Various types of scanning are implemented for efficient iterative analysis. An preferred technique which allows exhaustive signature scanning without requiring a comprehensive download of the signature data is described with reference to FIG. 4D above. Other scanning techniques are also provided for iterative virus detection. For example, techniques for the determination of whether a macro includes a virus can be modularized or divided into a plurality of functions which can be performed by separate virus detection objects. To explain, in the detection of known and unknown viruses in macros, combinations of suspect instructions can be used in the determination of whether a file includes a virus. Specifically, a macro that includes both a first suspect instruction and a second suspect instruction can be determined to include an unknown (or known) virus. Thus, in accordance with the present invention, separate virus detection objects are provided to first detect whether and which of several targeted files include a first suspect instruction, and then to determine whether those targeted files that include the first suspect instruction also include the second suspect instruction to detect a virus. To produce a first virus detection object the IVDM 450a operates with the scanning module 454 and the virus rules module 458 to obtain the routines and data required for the detection of the first suspect instruction. After transmission of the first virus detection object from the virus detection server 400 to the

client 300 and execution by the client 300, identification of those files that include the first suspect instruction can be identified in the results transmitted to the virus detection server 400. Alternatively, the file identifiers can remain at the client 300 and the result could indicate which suspect instruction was identified. In either case, the virus detection server 400 can use the results to produce an additional virus detection object to determine whether the second suspect instruction is present." (col. 19, line 39 - col. 20, line 6)

Appellant respectfully disagrees with this assertion. After reviewing the above excerpt, and the remaining Chen reference, it is clear that Chen fails to disclose, teach, or even suggest the specific assignment of the "identifier by the application" (emphasis added), let alone such functionality applied to an application program-process specific identifier, as claimed. Only appellant teaches and claims such a feature.

Yet again, the anticipation criterion has simply not been met by the Chen reference, in view of the stark deficiencies noted above. A notice of allowance or a specific prior art showing of such claimed features, in combination with the remaining claim elements, is respectfully requested.

*Group #6: Claims 19-20*

With respect to the present group, the Examiner relies on the following excerpts from Chen to make a prior art showing of appellant's claimed "virus detection actions [that] are selected by determining a category associated with the process based on the identifier, and selecting a set of virus detection actions based on the determined category."

"Similar to the scanning module 454, the virus pattern module 456 and virus rules module 458 respectively include virus signatures and rules that can be used in the detection of viruses. As with the routines described in connection with the scanning module 454, the patterns and rules are provided to facilitate separate access. Thus, for example, the file signatures in the virus pattern module 456 corresponding to one type of file can be separated from the virus signatures

corresponding to a second file type. Similarly, the rules in the virus rules module 458 corresponding to one detection criteria can be separated from the virus rules that apply to a second detection criteria. As with the routines in the scanning module 454, conventional indexing and sorting techniques can be used to provide separate access to the patterns and rules. Of course, a plurality of signatures or rules could apply to a particular indexing field. For example, several signatures would correspond to the indexing field .exe and thus would be included, subject to other indexing limitations, in the virus signatures corresponding to such scanning conditions.

In addition to providing routines and corresponding signatures or rules that separately accessible and thus amenable to tailoring according to the assessed scope and risk presented at the client 300, the virus scanning stage is provided such that scanning can be undertaken in iterations.

Preferably, information such as that provided in the exemplary data table 475 is provided in memory 414 for access by the IVDM 450a in the selection of virus scanning and treatment routines and, more specifically, in the production of virus detection and treatment objects. Assuming that, either by iterative object determination in the scope and risk assessment stages, or by user input, or by predetermined settings, that only files type viruses corresponding to a given platform I are targeted for scanning, the target would only be scanned for viruses such as viruses A, C, and E. The scanning routines are provided in the scanning module 454 and are indexed for access. Additionally, virus signatures are provided in the virus pattern module 456 and are indexed for access. Thus, using information such as that shown in the data table columns, the appropriate scanning routines for detecting file type viruses and virus signatures corresponding to viruses A, C and E are accessed. Although a virus detection object including full signatures corresponding to these three selected viruses could be provided in accordance with the present invention, a technique is provided which allows a further reduction in the amount of information required for transmission to the client 300 in order to detect viruses." (col. 12, lines 12-35; and col. 13, lines 1-23)

Again, Chen fails to even suggest any sort of virus detection action selected based on application program-specific identifiers, let alone "determining a category associated with the process based on the [application program-specific] identifier, and selecting a set of virus detection actions based on the determined category."

The anticipation criterion has simply not been met by the Chen reference, in view of the stark deficiencies noted above. A notice of allowance or a specific prior art

showing of such claimed features, in combination with the remaining claim elements, is respectfully requested.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

NA11P003/00.069.01

- 21 -



**VIII APPENDIX OF CLAIMS (37 C.F.R. § 41.37(c)(1)(viii))**

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Amended) A method for on-access computer virus scanning of files in an efficient manner, comprising the steps of:
  - (a) identifying a process for accessing files and selecting virus detection actions based at least in part on the identified process if no identifier is assigned thereto;
  - (b) assigning an identifier to the process if no identifier is assigned thereto;
  - (c) selecting virus detection actions based at least in part on the identifier if existent; and
  - (d) performing the virus detection actions on the files;
  - (e) wherein the process is associated with an application program, and different identifiers are assigned to different application programs so that the virus detection actions are tailored for the processes associated with the application programs.
2. (Original) The method as recited in claim 1, wherein the identifier is cleared upon the occurrence of a predetermined event.
3. (Original) The method as recited in claim 2, wherein the identifier is reused after being cleared.
4. (Original) The method as recited in claim 2, wherein the event is the termination of an application.
5. (Original) The method as recited in claim 4, wherein the identifier is assigned by the application.

6. (Original) The method as recited in claim 4, wherein the application is adapted for executing the process.
7. (Previously Amended) A computer program product for on-access computer virus scanning of files in an efficient manner, comprising:
  - (a) computer code for identifying a process for accessing files and selecting virus detection actions based at least in part on the identified process if no identifier is assigned thereto;
  - (b) computer code for assigning an identifier to the process if no identifier is assigned thereto;
  - (c) computer code for selecting virus detection actions based at least in part on the identifier if existent; and
  - (d) computer code for performing the virus detection actions on the files;
  - (e) wherein the process is associated with an application program, and different identifiers are assigned to different application programs so that the virus detection actions are tailored for the processes associated with the application programs.
8. (Original) The computer program product as recited in claim 7, wherein the identifier is cleared upon the occurrence of a predetermined event.
9. (Original) The computer program product as recited in claim 8, wherein the identifier is reused after being cleared.
10. (Original) The computer program product as recited in claim 8, wherein the event is the termination of an application.
11. (Original) The computer program product as recited in claim 10, wherein the identifier is assigned by the application.
12. (Original) The computer program product as recited in claim 10, wherein the application is adapted for executing the process.

13. (Previously Amended) A system for on-access computer virus scanning of files in an efficient manner, comprising:
- (a) logic for identifying a process for accessing files and selecting virus detection actions based at least in part on the identified process if no identifier is assigned thereto;
  - (b) logic for assigning an identifier to the process if no identifier is assigned thereto;
  - (c) logic for selecting virus detection actions based at least in part on the identifier if existent; and
  - (d) logic for performing the virus detection actions on the files;
  - (e) wherein the process is associated with an application program, and different identifiers are assigned to different application programs so that the virus detection actions are tailored for the processes associated with the application programs.
14. (Original) The system as recited in claim 13, wherein the identifier is cleared upon the occurrence of a predetermined event.
15. (Original) The system as recited in claim 14, wherein the identifier is reused after being cleared.
16. (Original) The system as recited in claim 14, wherein the event is the termination of an application.
17. (Original) The system as recited in claim 16, wherein the identifier is assigned by the application.
18. (Original) The system as recited in claim 16, wherein the application is adapted for executing the process.
19. (Previously Presented) The method as recited in claim 1, wherein the virus detection actions are selected by determining a category associated with the process based on

the identifier, and selecting a set of virus detection actions based on the determined category.

20. (Previously Presented) The method as recited in claim 19, wherein the identifier reflects a risk level associated with the application program, and a plurality of categories each have virus detection actions tailored for an associated risk level.

**IX APPENDIX LISTING ANY EVIDENCE RELIED ON BY THE  
APPELLANT IN THE APPEAL (37 C.F.R. § 41.37(c)(1)(ix))**

There is no such evidence.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P003).

Respectfully submitted,

By: \_\_\_\_\_

Kevin J. Zilka

Reg. No. 41,429

Date: \_\_\_\_\_

11/6/67

Zilka-Kotab, P.C.  
P.O. Box 721120  
San Jose, California 95172-1120  
Telephone: (408) 971-2573  
Facsimile: (408) 971-4660

NAI1P003/00.069.01

- 27 -